UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/800,378	03/05/2001	Joel De La Garza	SECU0003	3317

22862 7590 09/28/2004

GLENN PATENT GROUP
3475 EDISON WAY, SUITE L
MENLO PARK, CA 94025

EXAMINER	
ADAMS, JONATHAN R	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 09/28/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/800,378	GARZA, JOEL DE LA	
	Examiner	Art Unit	
	Jonathan R Adams	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 May 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☐ Claim(s) _____ is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *8* is/are allowed.

6)☒ Claim(s) *1-7 and 9-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 7 and 10 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

3. Claim 7 recites the limitation "each host" in line 4. There is insufficient antecedent basis for this limitation in the claim.

4. Claim 10 recites the limitation "the timestamps" in line 13. There is insufficient antecedent basis for this limitation in the claim.

5. Claims 11-13 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 11 uses the term “optionally” when listing the claimed limitations. It is unclear whether these limitations should be included in the claimed subject matter. Claims 12 and 13 are rejected as being dependent on a rejected base claim.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

7. Claims 1-3 and 9 rejected under 35 U.S.C. 102(a) as being anticipated by SystemSafe Online Backup Solutions.

8. As to claim(s) 1:

SystemSafe teaches a data collection/aggregation system for aiding victim machines comprising:

Mechanism for remotely collecting client data / Online Backup Solution (Page 1, Line 1, SystemSafe)

Mechanism for a victim machine for automatically verifying content received from victim machine / Transmission error checking (Page 4, Line 6, SystemSafe)

9. As to claim(s) 2:

Forensic evidence aggregator / Data backup center (Page 1, Col 3, Line 11, SystemSafe)

An image generation system / Full system backup (Page 2, Col 1, Line 15, SystemSafe)

Bootable image containing a forensic evidence collection suite / SystemSafe application (Page 1, Col 3, Line 6, SystemSafe)

10. As to claim(s) 3:

A set of scripts that gather from victim machine any of: network configuration, system architecture, media device configuration / Hassle free backup automatically starts whenever an internet connection is detected (Page 2, Col 1, Line 1, SystemSafe)

11. As to claim(s) 9:

Running machine from secure boot disk / standard client computer hard drive for full system backup (Page 2, Col 1, Line 15, SystemSafe)

Secure boot disk operating victim machine to produce first hash of said victim machine contents / standard IP (Page 4, Line 23, SystemSafe) checksum

Victim machine streaming contents to a remote location where they are securely stored / transmission sends data to offsite secure data servers (Page 1, Col 1, Line 25, SystemSafe)

Victim machine contents are captured at remote location performing second hash and comparison of first and second hash / standard IP (Page 4, Line 23, SystemSafe) checksum verification

Claim Rejections - 35 USC § 103

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to

> be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

13. Claim 4 rejected under 35 U.S.C. 103(a) as being unpatentable over SystemSafe in view of Workstation NT Recovery Tips.

As to claim(s) 4:

14. SystemSafe teaches a data collection/aggregation system for aiding victim machines. SystemSafe does not explicitly teach the use of a set of scripts generating a boot disk/image from a machine kernel after victimization. Workstation NT Recovery Tips teaches scripts to generate and use of boot disks for use with collected backup data for a victim machine (Page 1, Line 1). It would have been obvious to a person of ordinary skill in the art at the time of invention to use a boot disk as in Workstation NT Recovery Tips with the invention taught by SystemSafe. One of ordinary skill in the art would have been motivated to use a boot disk as in Workstation NT Recovery Tips with the invention taught by SystemSafe because in the event of a total system victimization/failure where it is not possible to boot from the hard disk it is necessary to boot from another device.

15. Claims 5 and 6 rejected under 35 U.S.C. 103(a) as being unpatentable over SystemSafe in view of Workstation NT Recovery Tips in further view of Introduction to SSL.

As to claim(s) 5:

16. SystemSafe as modified above teaches a remote server data collection/aggregation/backup system for aiding client victim machines. SystemSafe does not teach the use of a set of scripts that generate a one-use certificate for authentication and authorization that allow single connection to aggregation server from victim machine. Introduction to SSL teaches the use of scripts to generate that allow single connection to aggregation server from victim machine authentication/ authorization certificates for use client-server communications (Page 2, Lines 1-18, Intro to SSL). It would have been obvious to a person of ordinary skill in the art at the time of invention to use SSL for secure client-server communication in the invention of SystemSafe as modified above. One of ordinary skill in the art would have been motivated to use SSL for secure client-server communication in the invention of SystemSafe as modified above because SSL is a universally accepted Internet secure communications protocol and therefore has a beneficially pre-established infrastructure.

17. As to claim(s) 6:

An SSL server that restricts connections based upon verification of a certificate by a third party / Server checks client certificate, trusted certificate authority (Page 2, Lines 6-12, Intro to SSL)

18. Claim 10 rejected under 35 U.S.C. 103(a) as being unpatentable over SystemSafe in view of Workstation NT Recovery Tips in further view of

Introduction to SSL in further view of "Windows NT 4.0 Troubleshooting Guide" (hereafter referred to as WINNT).

19. SystemSafe as modified above teaches a data collection/aggregation system for aiding victim machines running under WINNT (Page 2, Col 2, Line 3, SystemSafe) using one-time SSL certificates and third party certificate authorities including message digest algorithms (Page 3, Introduction to SSL) and copying contents of victim machine over a secure channel to server (Page 1, Col 1, Line 25, SystemSafe). System safe does not teach Windows NT hardware architecture auto-detection capabilities. WINNT teaches the Windows NT hardware architecture auto-detection capabilities for networking and drive configurations (Page 2, Line 15, WINNT). It would have been obvious to a person of ordinary skill in the art at the time of invention to use the WINNT configuration settings in the Windows NT environment listed in SystemSafe as an optional operating system. One of ordinary skill in the art would have been motivated to use the WINNT configuration settings in the Windows NT environment listed in SystemSafe as an optional operating system because these configurations are necessary to provide the services listed in SystemSafe.

20. SystemSafe further does not teach the use of a read-only boot disk. The examiner takes official notice as to the WINNT ability for write protecting hard and floppy drives and folders contained within. It would have been obvious to a person of ordinary skill in the art at the time of invention to write protect the drive. One of ordinary skill in the art would have been motivated to write protect the drive in use because this prevents unauthorized tampering of the boot sequence.

Examples include write protected BIOS flash memory, write-protected bootable floppy disks by means of the write-protection tab, and write-protecting files, folders, and drives in WINNT corresponding to boot sequence system program code.

Allowable Subject Matter

21. Claim 8 is allowed.

22. The following is an examiner's statement of reasons for allowance: the claimed subject matter of claim 8 is considered to be novel, including:

- Incident response team entering relevant data into script to generate a kernel boot image for victim machine
- Incident response team providing client with one time password for on-line signing authority.
- Client accessing/downloading kernel boot image
- Sending victim machine data and hash of data on secure connection to be stored on an aggregation server

23. Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

24. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jonathan R Adams whose telephone number is (571)272-3832 after 10/04. The examiner can normally be reached on Monday – Friday from 10am to 6pm.

25. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse, can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100